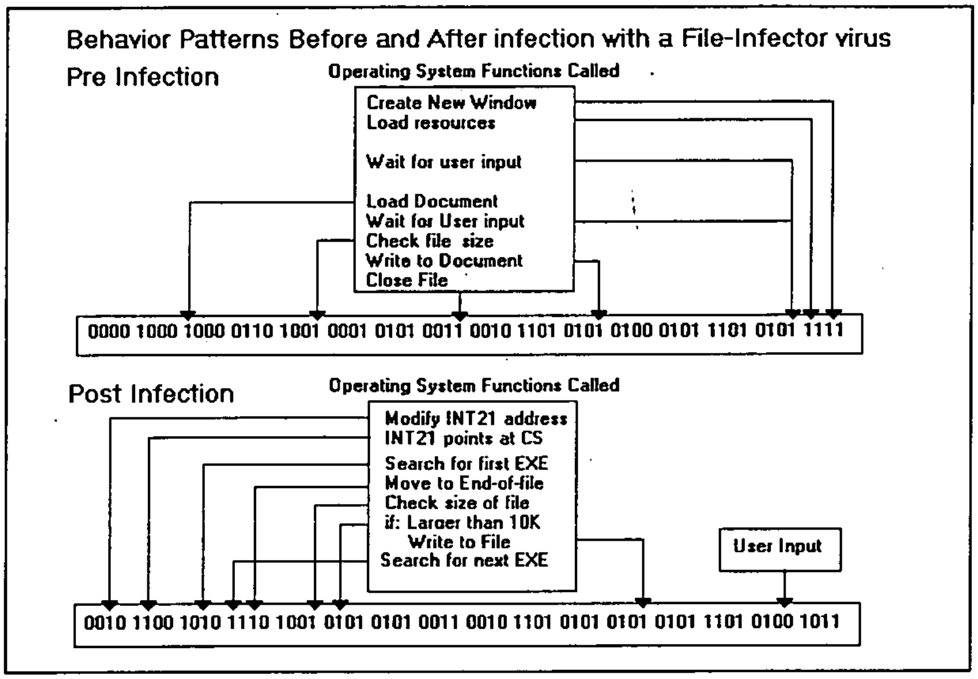
Behavior Patterns Before and After infection with a File-Infector virus
Pre Infection
Operating System Functions Called
Create New Window
Load resources
Wait for user input
Load Document
Wait for User input
Check file size
Write to Document
Close File
0000 1000 1000 0110 1001 0001 0101 0011 0010 1101 0101 0100 0101 1101 0101 1111
Post Infection
Operating System Functions Called
Modify INT21 address
INT21 points at CS
Search for first EXE
Move to End-of-file
Check size of file
if: Laroer than 10K
Write to File
Search for next EXE
User Input
0010 1100 1010 1110 1001 0101 0101 0011 0010 1101 0101 0101 0101 1101 0100 1011

FIG. 1

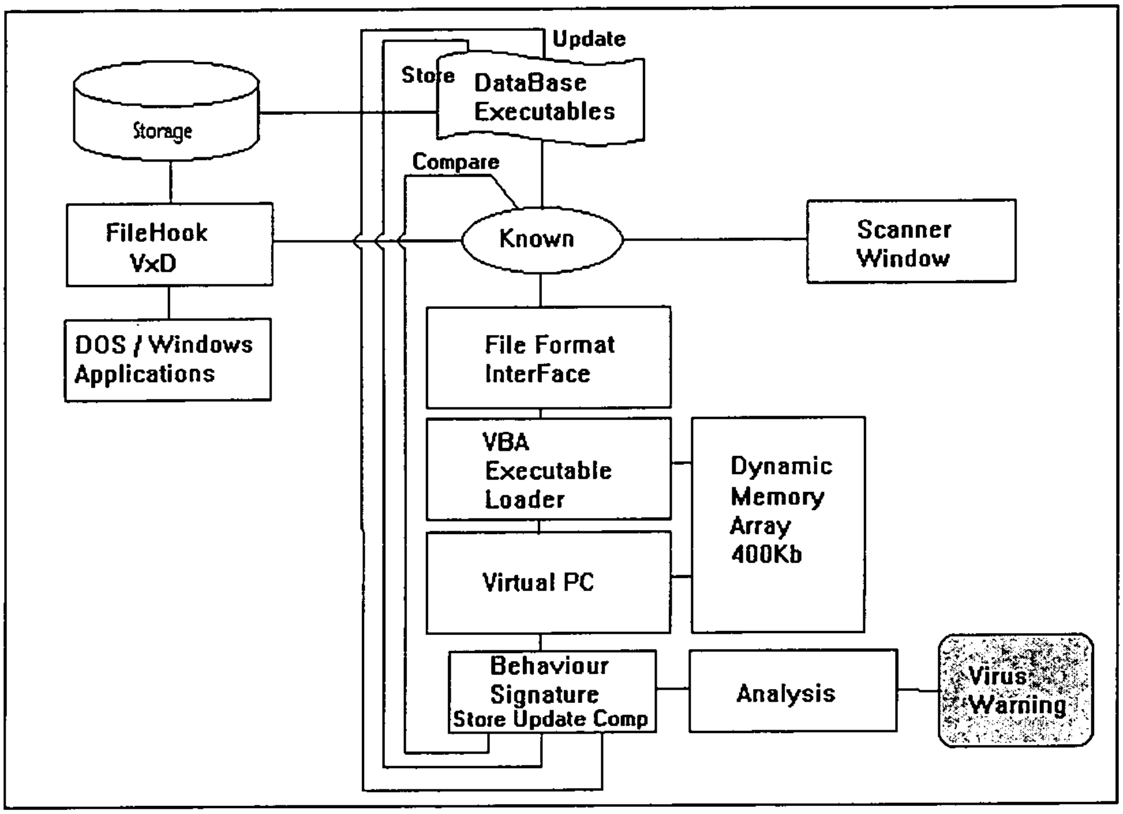
Update
Store
DataBase Executables
Storage
Compare
FileHook VxD
Known
Scanner Window
DOS / Windows Applications
File Format InterFace
VBA Executable Loader
Dynamic Memory Array 400Kb
Virtual PC
Behaviour Signature
Store Update Comp
Analysis
Virus Warning

FIG. 2

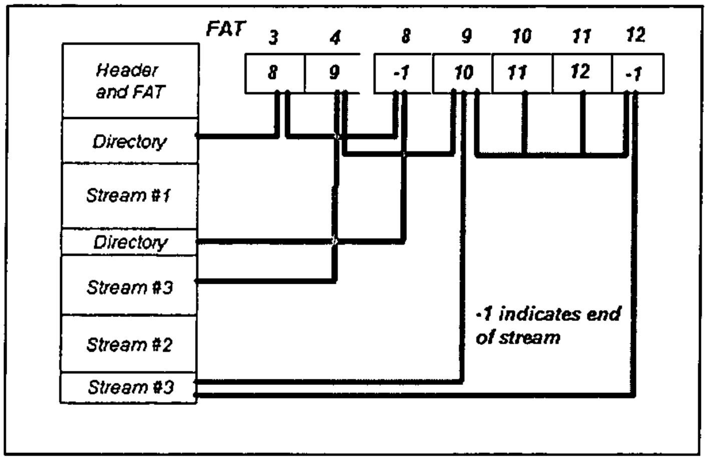
FAT
3
4
8
9
10
11
12
8
9
-1
10
11
12
-1
Header and FAT
Directory
Stream #1
Directory
Stream #3
Stream #2
Stream #3
-1 indicates end of stream

FIG. 3

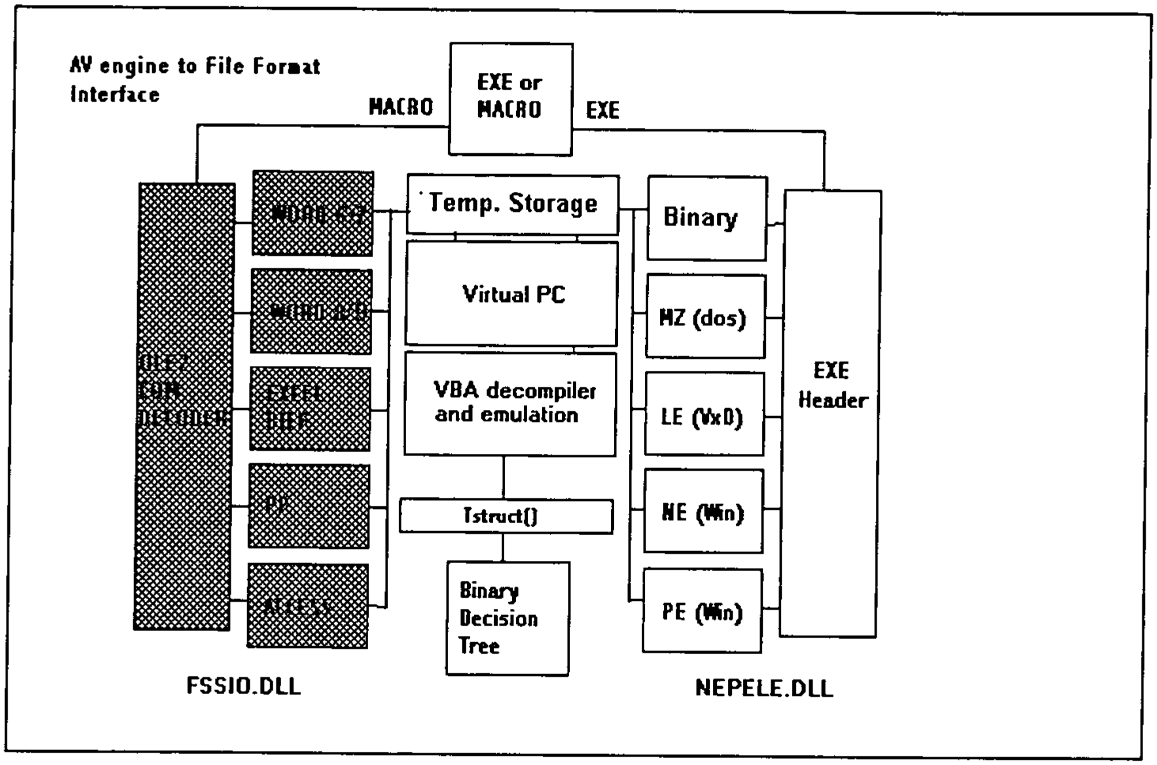
AV engine to File Format Interface
MACRO
EXE or MACRO
EXE
OLE2 COM DECODER
WORD 6/7
WORD 2.0
EXCEL
PP
ACCESS
Temp. Storage
Virtual PC
VBA decompiler and emulation
Tstruct()
Binary Decision Tree
Binary
MZ (dos)
LE (VxD)
NE (Win)
PE (Win)
EXE Header
FSSIO.DLL
NEPELE.DLL

FIG. 4

V80X86

MEMORY MAPS FOR BINARY COM AND EXE FILES

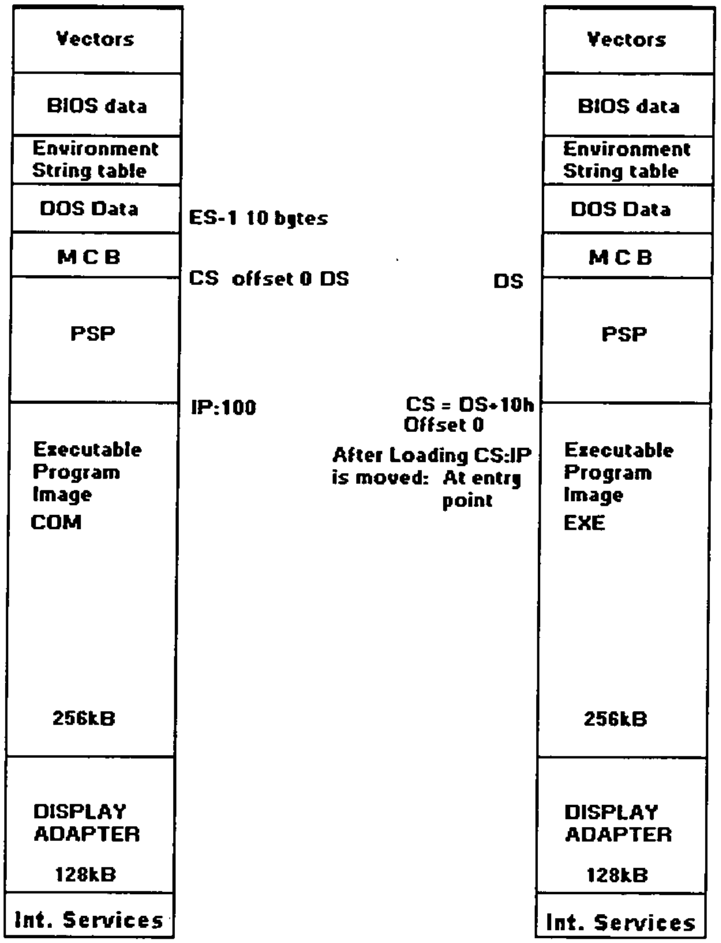

FIG. 5

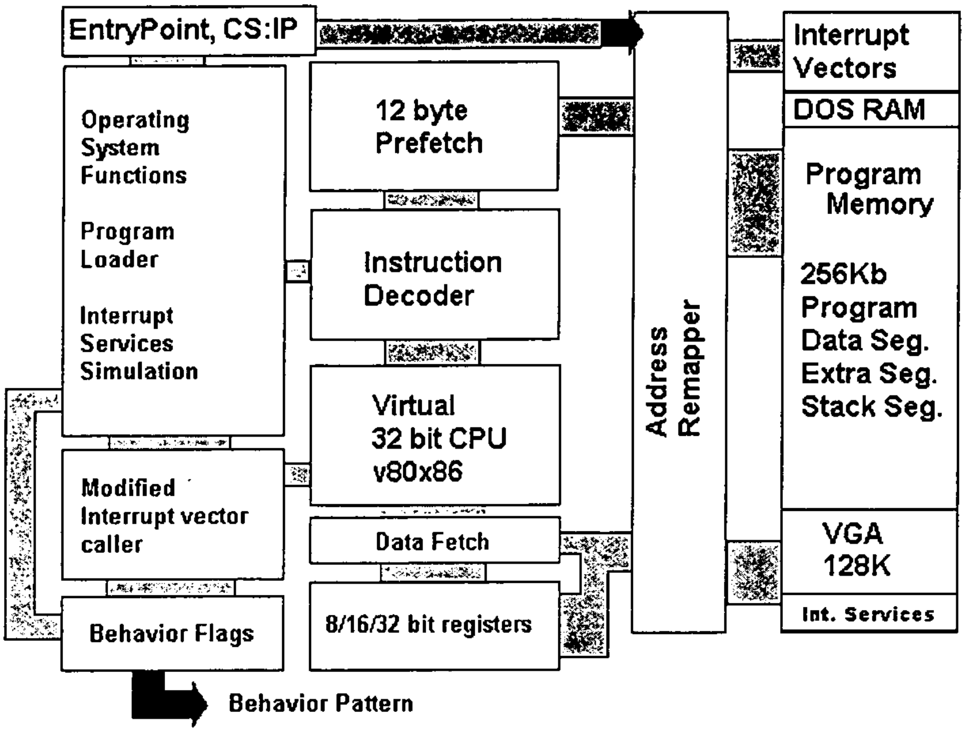
EntryPoint, CS:IP
Operating System Functions
Program Loader
Interrupt Services Simulation
12 byte Prefetch
Instruction Decoder
Virtual 32 bit CPU v80x86
Modified Interrupt vector caller
Data Fetch
Behavior Flags
8/16/32 bit registers
Behavior Pattern
Address Remapper
Interrupt Vectors
DOS RAM
Program Memory
256Kb Program Data Seg. Extra Seg. Stack Seg.
VGA 128K
Int. Services

FIG. 6